

WHAT IS CLAIMED IS:

1. A method for flexible and secure transmission of digital content to an end user device, the method comprising the steps of:
 - (a) providing a control center for controlling access to the digital content by the end user device;
 - (b) transmitting scrambled digital content to a first end user device by a second end user device, such that said second end user device cannot play back said scrambled digital content;
 - (c) connecting said second end user device to said control center; and
 - (d) transmitting a permission message to said second end user device by said control center, such that said second end user device is able to unscramble said scrambled digital content to form unscrambled digital content.
2. The method of claim 1, wherein step (b) includes the steps of:
 - (i) transmitting a first set of information for decoding said scrambled digital content to said second end user device; and
 - (ii) permitting said second end user device to access said first set of information only if said permission message is given to said second end user device.
3. The method of claim 2, wherein said first set of information is distributed with said scrambled digital content.
4. The method of claim 2, wherein said first set of information is distributed by said control center.
5. The method of any of claims 2-4, wherein step (d) includes the step of contacting said control center by said second end user device to receive said permission message.
7. The method of any of claims 2-5, wherein said first set of information includes an address of said control center.
8. The method of claim 1, wherein said first and said second end user devices

belong to a group of a plurality of end user devices, such that said permission message is sent to each end user device belonging to said group.

9. The method of claim 8, wherein membership in said group is at least partially determined according to communication between said end user devices.

10. The method of claim 9, wherein step (d) further comprises the step of transmitting a token from said first end user device to said second end user device, for including said first and said second end user devices in said group.

11. The method of claim 10, wherein the step of transmitting said token is performed repeatedly for the plurality of end user devices in the group until a limit is reached.

12. The method of claim 11, wherein said limit is determined according to a number of end user devices in the group, such that if said number of end user devices exceeds a maximum permitted number, steps (b) and (d) are not performed for an additional end user device.

13. The method of claim 12, wherein said limit is determined according to at least one reasonableness rule.

14. The method of claim 11, wherein said limit is determined according to at least one reasonableness rule and wherein said at least one reasonableness rule restricts a number of copies of said scrambled digital content operable with said token.

15. The method of claim 14, wherein when said limit is reached, at least one of steps (b) and (d) is not performed.

16. The method of claims 14 or 15, wherein said at least one reasonableness rule requires at least said first end user device to wait for a predetermined period before transferring said scrambled digital content to an additional end user device in the group.

17. The method of any of claims 14-16, wherein said at least one reasonableness rule

requires at least said first end user device to wait for a predetermined period before transferring said scrambled digital content to an additional end user device in the group.

17. The method of any of claims 14-16, wherein said at least one reasonableness rule requires said second end user device to wait for a predetermined period before transferring said scrambled digital content to an additional end user device in the group, said predetermined period being greater for said second end user device than for said first end user device.

18. The method of claims 14-17, wherein said period is at least partially determined according to a period of time.

19. The method of claims 14-18, wherein said period is at least partially determined according to operation of said end user device a minimum number of times.

20. The method of claim 8, wherein membership in said group is at least partially determined according to said control center, such that if said group has more than a predetermined number of end user devices as members, said control center blocks receipt of said permission message by members of said group.

21. A method for securing digital content for transmission to an end user device, comprising:

- (a) providing a control center for controlling access to the digital content by the end user device;
- (b) transmitting scrambled digital content to the end user device, such that the end user device cannot play back said scrambled digital content;
- (c) transmitting a PECM (personal ECM) to the end user device by said control center, said PECM being specific to the end user device; and
- (d) unscrambling said scrambled digital content by the end user device according to said PECM.

22. The method of claim 21, wherein step (c) further comprises the steps of:

- (i) transmitting a first set of information in an ECM (entitlement control message) for decoding said scrambled digital content to the end user device;

- (ii) permitting the end user device to access said first set of information only if an entitlement management message (EMM) is given to the end user device and said EMM indicates that the end user device is permitted to use said ECM; and
 - (iii) unscrambling said scrambled digital content by the end user device according to said first set of information.
23. The method of claim 22, wherein said EMM is transmitted by said control center.
24. The method of claims 22 or 23, further comprising the step of:
- (iv) replacing said ECM with said PECM for unscrambling said scrambled digital content by the end user device.
25. The method of any of claims 22-24, wherein said first set of information includes at least one instruction for generating a code word, such that step (ii) includes the steps of:
- (1) generating said code word according to said at least one instruction; and
 - (2) unscrambling said scrambled digital content according to said code word.
26. The method of any of claims 21-25, further comprising the step of:
- (e) permanently associating said PECM with said scrambled digital content to permit unscrambling of said scrambled digital content by the end user device.
27. The method of claim 26, further comprising the steps of:
- (f) transmitting said scrambled digital content with said ECM from a first end user device to a second end user device;
 - (g) receiving a specific PECM by said second end user device from said control center; and
 - (h) unscrambling said scrambled digital content by said second end user device only after receiving said specific PECM.
28. The method of claim 27, wherein step (g) includes the steps of:
- (i) transmitting payment to said control center; and
 - (ii) transmitting said PECM by said control center only after receiving payment.

29. A system for securing digital content for transmission, comprising:
- (a) an end user device for receiving scrambled digital content and for unscrambling said scrambled digital content for playing back the digital content;
 - (b) a broadcast unit for transmitting said scrambled digital content to said end user device;
 - (c) a permission message generator for generating a permission message for transmission to said end user device, such that said end user device unscrambles said scrambled digital content only after said permission message is at least received by said end user device, said permission message being specific for said end user device; and
 - (d) a subscription management system for controlling said permission message generator to determine whether said permission message is generated.
30. The system of claim 29, further comprising:
- (e) a network for connecting said end user device, said broadcast unit, said permission message generator and said subscription management system.
31. The system of claims 29 or 30, wherein said permission message generator sends said permission message to said subscription management system, and said subscription management system transmits said permission message to said end user device.
32. The system of any of claims 29-31, wherein said permission message generator further comprises:
- (i) an ECM (entitlement control message) generator for generating an ECM, said ECM forming a portion of said permission message; and
 - (ii) a PECM (personalized ECM) generator for generating a PECM, said PECM being specific to said end user device, said PECM forming another portion of said permission message.
33. The system of claim 32, wherein said end user device further comprises a security module for receiving said ECM and said PECM, and for unscrambling said scrambled digital content for playing back the digital content upon receipt of at least one of said ECM and said PECM.

34. The system of claim 33, wherein said security module further comprises a renewable security submodule, said renewable security submodule being removable and replaceable.

35. The system of claim 34, wherein said renewable security submodule comprises a smartcard.

36. The system of any of claims 33-35, wherein said security module features a limited number of slots for being associated with a plurality of ECMs, such that if said limited number of slots are used, a PECM corresponding to at least one stored ECM must be received before an additional ECM is received by said end user device.

37. The system of claim 36, wherein information concerning said slots is stored on said security module.

38. The system of any of claims 35-37, further comprising a smartcard reader for reading said smartcard, said smartcard reader being separate from said end user device, such that data produced by said smartcard is readable by said smartcard reader, including data resulting from said slots, said data being readable as a coded reply.

39. A method for unscrambling scrambled content before display, the scrambled content being digital data and the unscrambled content being displayed as an analog signal, the method comprising the steps of:

- (a) unscrambling the scrambled content to form unscrambled content as digital data;
 - (b) converting said unscrambled content from digital data to an analog signal, such that steps (a) and (b) are performed immediately before said analog signal is displayed; and
 - (c) displaying said analog signal;
- wherein steps (a) and (b) are performed at physically separated locations connected by a secure channel.

40. A method for secure distribution of digital content between end user devices,

comprising:

- (a) receiving scrambled digital content by a first end user device;
- (b) receiving a permission message for unscrambling said scrambled digital content by said first end user device;
- (c) transferring said scrambled digital content directly from said first end user device to a second end user device; and
- (d) unscrambling said scrambled digital content by said second end user device only after said permission message is activated for said second end user device.

41. The method of claim 40, wherein at least said second end user device is in communication with a control center and said permission message is activated for said second end user device by said control center.

42. The method of claims 40 or 41, wherein said first and said second end user devices belong to a group of a plurality of end user devices, such that said permission message is sent to each end user device belonging to said group.

43. The method of claim 42, wherein membership in said group is at least partially determined according to communication between said end user devices.

44. The method of claim 43, wherein step (b) further comprises the step of transmitting a token from said first end user device to said second end user device, for including said first and said second end user devices in said group.

45. The method of claim 44, wherein the step of transmitting said token is performed repeatedly for the plurality of end user devices in the group until a limit is reached.

46. The method of claim 45, wherein said limit is determined according to a number of end user devices in the group, such that if said number of end user devices exceeds a maximum permitted number, steps (b) and (c) are not performed for an additional end user device.

47. The method of claim 46, wherein said limit is determined according to at least

one reasonableness rule.

48. The method of claim 45, wherein said limit is determined according to at least one reasonableness rule and wherein said at least one reasonableness rule restricts a number of copies of said scrambled digital content operable with said PECM.

49. The method of claim 48, wherein when said limit is reached, at least one of steps (b) and (c) is not performed.

50. The method of claims 48 or 49, wherein said at least one reasonableness rule requires at least said first end user device to wait for a predetermined period before transferring said scrambled digital content to an additional end user device in the group.

51. The method of any of claims 48-50, wherein said at least one reasonableness rule requires said second end user device to wait for a predetermined period before transferring said scrambled digital content to an additional end user device in the group, said predetermined period being greater for said second end user device than for said first end user device.

52. The method of claims 48-51, wherein said period is at least partially determined according to a period of time.

53. The method of claims 48-52, wherein said period is at least partially determined according to operation of said end user device a minimum number of times.

54. The method of claim 41, wherein membership in said group is at least partially determined according to said control center, such that if said group has more than a predetermined number of end user devices as members, said control center blocks receipt of said permission message by members of said group.

55. The method of any of claims 40-54, wherein step (d) comprises the steps of:
- (i) purchasing the digital content; and
 - (ii) activating said permission message for said second end user device.

56. The method of claim 40, wherein said permission message is operative only by said first end user device, such that if said permission message is transferred to said second end user device by said first end user device, said permission message cannot be used by said second end user device.

57. A secure precision digital to analog converter, comprising:

- (a) an encryption engine;
- (b) a digital to analog converter for accepting input from said encryption engine for performing digital to analog conversion, said input including encrypted digital content and a key for decrypting said encrypted digital content; and
- (c) a secure channel for connecting said encryption engine to said digital to analog converter, wherein said encryption engine is physically separated from said digital to analog converter.

58. The converter of claim 57, wherein said digital to analog converter further comprises:

- (i) a plurality of weighted resistors; and
- (ii) a plurality of control registers for controlling a weight of each resistor, said plurality of control registers determining said weight according to said key.

59. The converter of claim 58, wherein at least one weight of said weighted resistors is a fractional weight.

60. The converter of any of claims 57-59, further comprising an additional channel for transferring said encrypted digital content, such that said secure channel transfers said key.

61. The converter of claim 60, wherein said additional channel and said secure channel share identical physical lines.

62. A method for secure transmission of scrambled content to an end user device, the scrambled content comprising digital data, the method comprising the steps of:

- (a) transmitting the scrambled content to the end user device;
- (b) receiving a permission message by the end user device;

- (c) unscrambling the scrambled content to form unscrambled content as digital data only after receiving said permission message by the end user device;
- (d) converting said unscrambled content to rescrambled content;
- (e) unscrambling said rescrambled content when converting said content from digital data to an analog signal, such that steps (b) and (c) are performed immediately before said analog signal is displayed; and
- (f) displaying said analog signal.

63. A secure precision digital to analog converter.

64. A method for securely and precisely converting scrambled data to a final format for display, the steps of the method being performed within a secure device, the method comprising the steps of:

- (a) completely unscrambling the scrambled data to an unscrambled format of data; and
- (b) immediately converting said data in said unscrambled format to the final format for display, such that steps (a) and (b) are performed within the secure device, and such that said data in said unscrambled format is inaccessible externally to the secure device.

65. The method of claim 64, wherein converting scrambled data to the final format for display includes conversion of digital data to an analog signal.

66. The method of claims 64 or 65, wherein step (a) further comprises the steps of:
- (i) receiving the scrambled data;
 - (ii) unscrambling the scrambled data to a first unscrambled data;
 - (iii) rescrambing said first unscrambled data to form rescrambled data; and
 - (iv) unscrambling said rescrambled data to form said data in said unscrambled format of data.

67. The method of claim 66, wherein the scrambled data is distributed to a plurality of secure devices, and wherein steps (iii) and (iv) are performed according to a different scheme by each secure device.

68. The method of claim 67, wherein the step of rescrambling said first unscrambled data to form said rescrambled data is performed differently by each secure device for each unscrambling operation.

69. In a system for secure distribution of digital content, the system comprising a control center for distributing at least one key for unscrambling scrambled digital content and an end user device for receiving the scrambled digital content, a method for providing temporary access to received scrambled digital content, the method comprising the steps of:

- (a) sending a temporary key from the control center to the end user device, said temporary key being valid for a limited period of time;
- (b) receiving the scrambled digital content by the end user device; and
- (c) unscrambling the scrambled digital content by the end user device according to said temporary key, such that the end user device is only permitted to unscramble the scrambled digital content while said temporary key is valid.

70. The method of claim 69, further comprising the steps of:

- (d) receiving a permanent key by the end user device from the control center;
- (e) replacing said temporary key with said permanent key; and
- (f) unscrambling the scrambled digital content by the end user device according to said permanent key, such that the end user device has permanent access to the scrambled digital content.

71. A method for securing digital content for transmission to a plurality of end user devices, said plurality of end user devices being members of a group, the method comprising the steps of:

- (a) transmitting scrambled digital content to a first end user device, such that said first end user device cannot play back said scrambled digital content;
- (b) transmitting a PECM (personal ECM) to said first end user device, said PECM being specific to the group of end user devices;
- (c) transmitting said scrambled digital content from said first end user device to a second end user device, such that said second end user device cannot play back said scrambled digital content;

43

- (d) transmitting said PECM (personal ECM) to said second end user device; and
- (e) unscrambling said scrambled digital content by said first and said second end user devices according to said PECM.

72. The method of claim 71, wherein a control center controls access to the digital content by the group of end user devices, and wherein said PECM is sent at least to said first end user device by said control center.

73. The method of claims 71 or 72, wherein said PECM is sent from said first end user device to said second end user device.

74. The method of any of claims 71-73, wherein steps (c) and (d) are performed repeatedly for the plurality of end user devices in the group until a limit is reached.

75. The method of claim 74, wherein said limit is determined according to a number of end user devices in the group, such that if said number of end user devices exceeds a maximum permitted number, steps (c) and (d) are not performed for an additional end user device.

76. The method of claim 75, wherein said limit is determined according to at least one reasonableness rule.

77. The method of claim 74, wherein said limit is determined according to at least one reasonableness rule and wherein said at least one reasonableness rule restricts a number of copies of said scrambled digital content operable with said PECM.

78. The method of claim 77, wherein when said limit is reached, at least one of steps (c) and (d) is not performed.

79. The method of claim 78, wherein said at least one reasonableness rule requires at least said first end user device to wait for a predetermined period before transferring said scrambled digital content to an additional end user device in the group.

81. The method of claims 79 or 80, wherein said period is at least partially determined according to a period of time.

82. The method of claims 79 or 80, wherein said period is at least partially determined according to operation of said end user device a minimum number of times.

83. The method of claim any of claims 2-7, wherein said first set of information enables said unscrambled digital content to be permanently stored by said second end user device.

09044397 13400
FOIET 2647550